

Differential fault analysis

From Wikipedia, the free encyclopedia

Differential fault analysis is a type of side channel attack in the field of cryptography, specifically cryptanalysis. The principle is to induce *faults*—unexpected environmental conditions—into cryptographic implementations, to reveal their internal states.

For example, a smartcard containing an embedded processor might be subjected to high temperature, unsupported supply voltage or current, excessively high overclocking, strong electric or magnetic fields, or even ionizing radiation to influence the operation of the processor. The processor may begin to output incorrect results due to physical data corruption, which may help a cryptanalyst deduce the instructions that the processor is running, or what its internal data state is.^{[1][2]}

For DES and Triple DES, about 200 single-flipped bits are necessary to obtain a secret key.^[3]

References

- [^] Eli Biham, Adi Shamir: The next Stage of Differential Fault Analysis: How to break completely unknown cryptosystems (1996)
- [^] Dan Boneh and Richard A. DeMillo and Richard J. Lipton: On the Importance of Checking Cryptographic Protocols for Faults, Eurocrypt (1997)
- [^] Ramesh Karri, et al.: Fault-Based Side-Channel Cryptanalysis Tolerant Rijndael Symmetric Block Cipher Architecture (2002)

Retrieved from "http://en.wikipedia.org/wiki/Differential_fault_analysis"

Categories: Cryptography stubs | Cryptographic attacks

- This page was last modified on 21 February 2010 at 16:59.
 - Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. See Terms of Use for details.
- Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.